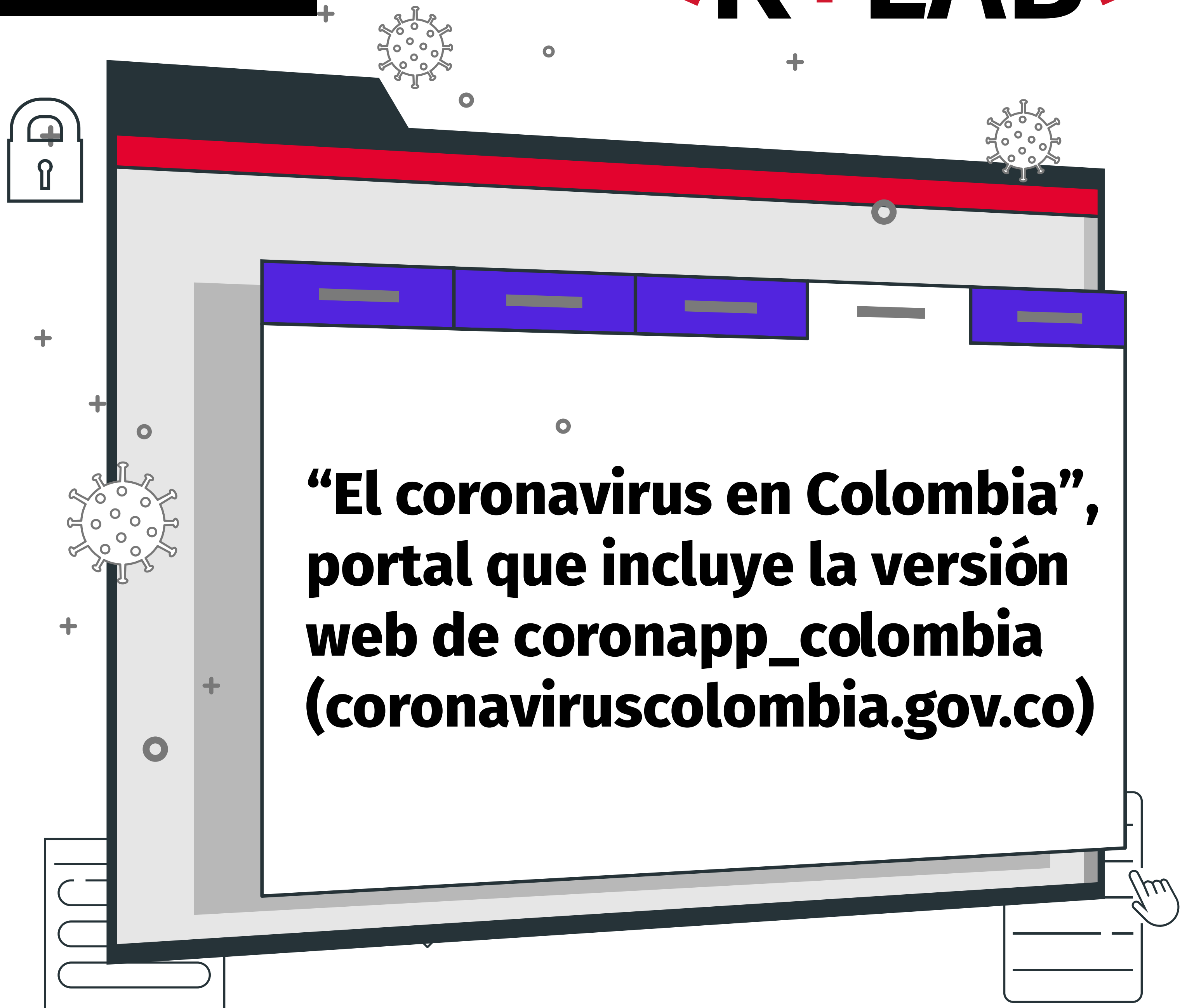
Análisis

<K+LAB>



"El coronavirus en Colombia", portal que incluye la versión web de coronapp_colombia (coronaviruscolombia.gov.co)

Este informe se basa en investigaciones que se hicieron en febrero del 2021 y que se volvieron a verificar en mayo 2021. Intentamos varias veces comunicarnos a través del MinTiC con la Presidencia, que aparece como encargada del sitio, pero no obtuvimos la reunión propuesta. Teniendo en cuenta que las vulnerabilidades no son severas y que de hecho las malas prácticas reportadas han sido previamente alertadas por el MinTIC en su documento sobre "Condiciones mínimas técnicas y de seguridad digital", decidimos publicar este análisis.

Contempla un análisis jurídico de la política de privacidad del sitio (parte 1) y un análisis técnico y no intrusivo de los formularios webs. Los resultados se presentan a través de dos tablas (partes 2 y 3 y anexos).

K

Fundación Karisma

1. Contexto y política de tratamiento de la información

1.1 Contexto

El sitio web "coronaviruscolombia.gov.co" es un portal del gobierno colombiano que ofrece información y acceso a algunos servicios relacionados con el coronavirus en el país. El portal incluye, entre otros, la versión web de la aplicación *CoronApp Colombia* que Fundación Karisma ya ha analizado en varias de sus versiones[1] y un formulario de autodiagnóstico. *Coronapp Colombia* se hizo "*disponible para web*" para el que "*tiene un número internacional o un celular antiguo*", de forma tal que pueda "*obtener [su] código QR de viajero*" como lo menciona el mismo sitio web[2]. Las finalidades expresadas en la política de privacidad del portal son las siguientes:

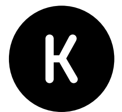
> "*La PRESIDENCIA DE LA REPÚBLICA recolectará, usará y tratará los datos personales de manera leal y lícita para para obtener información estadística, análisis de política pública, para poder emitir una respuesta por parte del Mecanismo de Comunicación Masiva, el despliegue de medidas de prevención y contención frente al COVID-19, específicamente para presentar recomendaciones a signos de alarma de afección respiratoria y riesgos en salud pública asociados al coronavirus COVID-19 y crear y mantener la base de datos de los usuarios del Mecanismo de Comunicación Masiva.*"[3]

El sitio web contiene:

1. Información vinculada con el Covid-19: *Acciones del Gobierno*, *Mitos y preguntas*, *Enlaces de interés*, *Líneas de atención, cifras, etc.*
2. Una página de registro y de conexión a CoronApp Colombia en su versión web[4].
3. Una página con un formulario de autodiagnóstico, que no necesita estar conectado a CoronApp Colombia ni ingresar datos personales que identifiquen a la persona directamente[5].
4. Un menú "*Denuncia virtual*" que re-dirige hacia la página de denuncia virtual de la Policía Nacional[6].

Esta última página, por ser un sitio externo, no hace parte de este análisis que se enfoca en los formularios de autodiagnóstico, de registro, de conexión y en las funcionalidades de la versión web de la CoronApp. Sin embargo nos preguntamos sobre la finalidad de este enlace en este contexto.

1 Fundación Karisma ha realizado varios análisis y publicado varios artículos sobre CoronApp Colombia. Dentro de ellos se pueden mencionar el primer análisis técnico (https://web.karisma.org.co/wp-content/uploads/2020/04/Informe-p%C3%Bablico-t%C3%A9cnico-CoronApp-v170320-1-1.pdf), el análisis de la evolución de los permisos (https://web.karisma.org.co/permisos-de-las-apps-de-covid-cuando-bajara-esta-curva/) y el análisis de la versión de la aplicación para teléfonos iPhone (https://web.karisma.org.co/coronapp-en-android-o-en-ios-cual-de-las-dos-hace-menos-mal-la-tarea-de-proteger-la-privacidad-de-las-personas/).
2 Ver "CoronApp disponible para web" en: https://coronaviruscolombia.gov.co/Covid19/index.html
3 https://coronaviruscolombia.gov.co/Covid19/politica-de-privacidad.html
4 https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html
5 Como por ejemplo, nombre, cédula o correo electrónico.
6 La página principal contiene un menú llamado "Denuncia virtual". Al hacer clic en el, uno es dirigido al sistema de denuncia virtual de la policía nacional (https://adenunciar.policia.gov.co/Adenunciar/Login.aspx?ReturnUrl=%2fadenunciar%2fdefault.aspx).



1.2 Política de privacidad / tratamiento de la información

La Presidencia de la República aparece, en la política de tratamiento de datos de *El Coronavirus en Colombia*[7] como responsable de tratamiento de datos. Sin embargo, cuando uno se registra para CoronApp Colombia web, el sitio pide aceptar la política de tratamiento de datos de CoronApp ubicada en el sitio web del Instituto Nacional de Salud (INS) (al día de la publicación de este informe este enlace ya no funciona[8]) y unos Términos y Condiciones en los cuales el INS aparece como responsable de tratamiento. La política de tratamiento de datos de *El Coronavirus en Colombia* está confeccionada a partir de fórmulas generales e incluso contradictorias. La Presidencia de la República como responsable del tratamiento de datos, cumple con el deber legal asociado a su publicación en tanto que recaba datos que identifican o hacen identificables a las personas. **Sin embargo, no se trata de una política que aclare varios de los aspectos sobre los que sería deseable tener claridad. Además parece que la parte de "CoronApp web" compite con la política de tratamiento de la información y los términos y condiciones de CoronApp_Colombia sin aclaración que permita entender cuando se aplica la una o la otra *sobre el suministro de los datos a terceras partes.***

No se advierte en la redacción de la política de privacidad los criterios (requisitos o situaciones) que son considerados por el responsable del tratamiento de la información y que habilitarían para el suministro o acceso de los datos personales por parte de terceros. No advierte limitaciones para su entrega a ciertas entidades públicas o entidades privadas. La fórmula para permitir acceso a entidades del sector público apunta, sin mayor contexto ni desarrollo, a la habilitación de toda autoridad que "en el ejercicio de sus funciones así lo requieran"[9].

No se precisan, ni se advierten los requisitos exigibles por parte de la Presidencia de la República a esos terceros para asegurar que aquellos cuentan a su vez, con políticas de tratamiento de datos que sean públicas, integrales, y que provean mecanismos de reclamo a las personas cuya información pueden llegar a tener en sus manos.

Sobre la transferencia y transmisión internacional de datos personales

Esta sección de la política de tratamiento de datos advierte que la Presidencia de la República deberá suscribir contratos con terceros cuando necesite enviar o transmitir datos "a uno o varios encargados ubicados fuera del territorio de la República de Colombia"[10]. Sin embargo, no se advierte, en un proceso de contextualización de esa fórmula genérica consagrada en la política de tratamiento de datos que, en efecto, el sistema transfiere datos a terceras partes de carácter privado fuera del país tales como Amplitude, Amazon, Google o CloudFlare, ubicadas en Estados Unidos (ver partes 2 y 3).

Recomendación: Sería conveniente que se describiera que el tratamiento de datos en El Coronavirus en Colombia actualmente incluye esa transferencia internacional, que debe constar en acuerdos que son anexos a la política y, por tanto, deberían ser públicos también.

7 https://coronaviruscolombia.gov.co/Covid19/politica-de-privacidad.html
8 https://www.ins.gov.co/Normatividad/PoliticasInstitucionales/politica-de-tratamiento-de-informacion-coronapp-colombia.pdf
9 Ver sección "autorización tratamiento datos personales".
10 Ver sección "transferencia y transmisión internacional de datos personales".

Sobre terceros que obran como "encargados" del tratamiento de datos

Utilizando fórmulas genéricas que no dan contexto concreto a *El Coronavirus en Colombia*, la Presidencia de la República contempla la posibilidad de que el tratamiento de datos pueda ocurrir a través de una tercera parte en el rol de "encargada del tratamiento". Sin embargo, no se describen quiénes pueden ser esas partes que obrarían como encargadas, cuáles son los propósitos que cumplirían en la cadena de intermediación del tratamiento de los datos, cuáles los deberes que tendrían esas partes a cargo, y qué derechos tiene la persona titular del dato en relación con éstas.

Del análisis realizado, parece que el Instituto Nacional de Salud y la Agencia Nacional Digital obran como encargados para Coronapp web (ver parte 3) y que la empresa "1doc3" obra como encargada para la funcionalidad de autodiagnóstico (ver parte 2),

Recomendación: La política de protección de datos debe ocuparse de estos terceros que desde el diseño de la aplicación parecen ser los "encargados" del tratamiento de datos y en ese contexto, los contratos deberían ser parte de esta política y hacerse públicos para conocimiento de las personas cuyos datos serán tratados por las empresas.

Sobre la obligatoriedad en el uso de CoronApp web

La política de tratamiento de datos es contradictoria al afirmar que la entrega de datos sensibles asociados a la salud de las personas - que la Ley 1581 de 2012 considera como sensibles - no es obligatoria[11], al tiempo que reitera que el principio de libertad que sustenta el ejercicio de la autonomía de la voluntad y que faculta a la persona a la entrega o no de los datos personales y, sin embargo, agrega que esto "no aplica en el caso de la CoronApp Colombia por mandato del artículo 10 de la ley 1581 de 2012"[12].

Muy a pesar del debate que pueda existir en torno a la aplicación conveniente del texto del artículo 10 de la Ley 1581 de 2012 y que ha sido también objeto de discusión en relación con la política de tratamiento de datos de la aplicación móvil de CoronApp, es importante poner de presente que a dicha obligación que busca limitar el ejercicio del derecho fundamental al *habeas data,* no se encuentra aparejado un ejercicio que presente al titular del dato las razones por las que, de manera proporcional y necesaria, su consentimiento no cuenta a la hora de usar CoronApp web.

Recomendación: Si se va a aplicar el artículo 10 de la Ley 1581 de 2012 se debe describir la justificación en la política de tratamiento de datos de manera clara en tanto que no existe mandato legal que obligue al uso de este tipo de tecnologías o herramientas.

Sobre la anonimización de los datos

Se prevé por la política que, una vez recolectados los datos "por regla general se utilizarán herramientas de anonimizarían (sic) para que no esté asociada o vinculada a una persona en particular". Y advierte además, que dicha regla general de anonimización podrá ser exceptuada "cuando [sea] rigurosamente necesario conocer la identidad del titular del dato"[13]. En la política de tratamiento de información de CoronApp_web

11 Ver sección "de la no obligatoriedad de suministrar datos sensibles relativos a la salud y de la responsabilidad reforzada".
12 Ver sección "principios relacionados con la recolección de datos personales".
13 Ver sección "datos anonimizados".

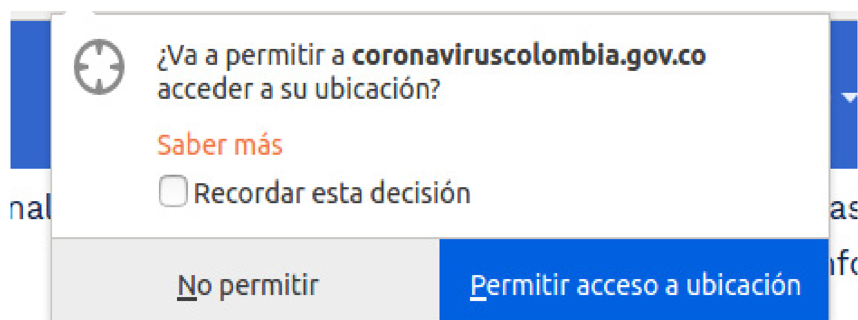
hay una formulación similar[14].

Además, los análisis que hemos hecho muestran que al menos los datos de la parte "conectada" de Coronapp Web, siendo asociada a los datos de registro (nombre, apellidos, tipo y número de documento, número de celular, correo electrónico), no son anónimos. Es decir, ya desde el inicio la regla se rompe confirmando que la ausencia de los criterios mencionados disminuyen la protección de manera injustificada.

Recomendación: Se deben describir los criterios del "rigurosamente necesario" que puede derivar en la desanonimización de los datos personales e indicar en esos casos cómo se protegen o mitigan los efectos nocivos para los derechos de las personas usuarias. Se debe revisar por qué la propia recolección de datos está haciéndose de forma desanonimizada e implementar los correctivos necesarios.

Sobre el acceso a la localización

Cuando uno llega en sitio web, el navegador pide el permiso para que el sitio pueda acceder a la ubicación:



Sin embargo, la política de privacidad del portal no menciona la finalidad de este acceso.
Recomendación: informar al usuario de la finalidad del acceso a la ubicación

Sobre la seguridad de la información

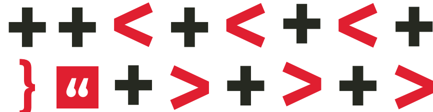
La política de tratamiento señala que cuenta con una política de seguridad y cita el enlace a la política de tratamiento de datos. Es decir, se cita a sí misma y en su texto, en todo caso, no desarrolla las acciones de mitigación de fuga de datos que serían emprendidas cuando sucedan brechas de seguridad de la información.

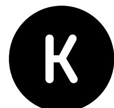
Recomendación: Siguiendo buenas prácticas internacionales se debería establecer que las personas serán notificadas cuando la seguridad de sus datos sea comprometida. Se deberían describir las acciones que se emprenderán por la parte responsable del tratamiento incluyendo el cumplimiento de las obligaciones de cara a la autoridad de protección de datos. Se debe informar sobre quién se encarga de revisar, evaluar y mejorar15 las condiciones de seguridad de la información que se recolecta a través de El Coronavirus en Colombia y para sus componentes como CoronApp web.

14 Ver páginas 8 y 9 de la política, parte "Datos anonimizados".
15 Ver sección "medidas de seguridad aplicadas al tratamiento de datos personales".

2 Tabla sintética del formulario de autodiagnóstico

Categoría	Descripción
URL	https://coronaviruscolombia.gov.co/Covid19/auto-diagnostico.html
Datos recolectados	Esta página permite hacer un auto-diagnóstico de riesgos de haber contraído el COVID-19. El formulario no necesita entregar datos personales que identifiquen directamente a la persona usuaria (cómo nombre, cédula, etc.). Sin embargo se recolectan datos sensibles relativos a los síntomas susceptibles de indicar una infección con COVID-19 y a los contactos eventuales de la persona con otras infectadas, y el análisis mostró que estos datos se transmiten asociados a varios identificadores de la persona usuaria [Anexo 1].
Hosting	El servidor web principal tenía en nuestro primer análisis la dirección IP 170.246.114.222 que pertenece a la empresa colombiana *Media Commerce Partners S.A.* ubicada en Pereira. Al día de esta publicación tiene la dirección IP 190.145.219.66 que pertenece a la empresa colombiana Telmex Colombia S.A. Sin embargo, el análisis nos permite afirmar que los datos personales del formulario no son transmitidos a una entidad del estado, ni a estas empresa, sino al dominio “amplitude.com” de la empresa Amplitude ubicada en Estados Unidos [Anexo 1]. Este dominio está vinculado con la empresa 1Doc3, también presente en la página. *Amplitude* contrató un servicio de hosting a *Amazon Technologies*, en Estados Unidos [Anexo 2]. **Ninguno de estas empresas (Media Commerce Partners, Telmex, 1Doc3, Amplitude y Amazon technologies) que participan o han participado en el tratamiento de los datos se mencionan en la política de privacidad.** **<u>Recomendación</u>: Cómo se explicó en la parte 1, la política de protección de datos debe reconocer este modelo de flujo de los datos personales puesto que indica que es una de estas empresas la encargada de tratamiento de datos y estas sub-contrataciones implican transferencia de datos personales a Estados Unidos lo que de acuerdo con la política tiene condiciones preestablecidas, aunque -cómo se explicó en la parte 1- éstas están pobremente descritas en las políticas de privacidad.**
Cifrado y autenticación	El portal usa de forma predeterminada el protocolo seguro HTTPS (HTTP+TLS) con un certificado de la empresa Go Daddy Inc.
Envío de los datos de autodiagnóstico	Los datos de autodiagnóstico transmitidos por los formularios se envían con el protocolo HTTPS y el método POST. Se transmiten únicamente a la URL “https://api.amplitude.com/”, esta misma es llamada por el dominio “1doc3.com”. Esto se debe a que todo el cuestionario de auto-diagnóstico es un elemento HTML externo al sitio original (iframe HTML) con dominio “1doc3.com”. Por lo cual pensamos que el encargado de tratamiento de los datos recolectados por este formulario es la empresa 1doc3, y que fue ésta última la que contrató con la empresa Amplitude que es la que recibe los datos a través de su dominio “amplitude.com”. [Ver Anexos 1 y 2] **<u>Recomendación:</u> igual que para la parte Hosting y en línea con lo descrito en la parte 1 de este informe.**
Tecnologías usadas y actualizaciones	El servidor web es un servidor con Microsoft Sharepoint con el framework Bootstrap [ver Anexo 3]. El análisis de las cookies internas muestra que muy probablemente se usa un balance de carga de tipo “F5 BIG-IP ASM” versión 11.4.0 o posterior [Ver Anexos 4 y 7]. **<u>Recomendación:</u> Es importante asegurarse de la actualización del servidor web y de todos sus componentes.**





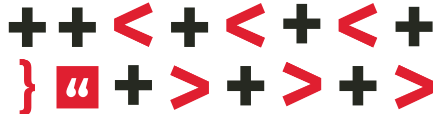
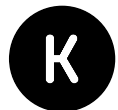
Protecciones adicionales	<u>**Recomendación**</u>: Se recomienda implementar protecciones adicionales, siguiendo los lineamientos de seguridad digital del MinTIC para los sitios web[16], en particular las siguientes, ya que nuestro análisis mostró que no están implementadas: • Cookies: habilitar los atributos de seguridad *Secure* y *HttpOnly*, en particular para la cookie "TS01bee912" que parece tener funcionalidades de seguridad vinculadas con el balance de carga ; • habilitar las cabeceras de seguridad[17].
Rastreo y cookies de terceros	En la página de auto-diagnóstico, además de las cookies internas, se instalan varias cookies asociadas a los dominios: 1doc3.com, facebook.com y al servicio *Google Analytics.* La cookie de Facebook está originada por el dominio "1doc3.com". También se puede mencionar un hecho extraño probablemente debido a un error técnico: se instalaban varias cookies internas vacías (problema técnico que parece haber sido resuelto). Finalmente, el elemento HTML del dominio "1doc3.com" (iframe) también genera solicitudes con transmisiones de identificadores hacia la sucursal publicitaria de Google, a través de su dominio "doubleclick.net" [ver Anexo 4]. <u>**Recomendación:**</u> **es importante evaluar la consecuencia de que se instalen cookies a las personas usuarias del sitio sobre todo en términos de rastreo publicitario. El Coronavirus en Colombia es un sitio del Estado que recoge información sensible y que parece tuvo cuidado de no crear espacios para la instalación de cookies de terceros, sin embargo, debido al uso de la herramienta de la empresa 1doc3 se termina instalando una cookie de Facebook. En caso de que esto no pueda evitarse se debería informar a las personas usuarias.**

16 *Condiciones mínimas técnicas y de seguridad digital del MinTIC* (Anexo 3 de la Resolución MinTIC 1519 del 2020).

17 Los lineamientos del MinTIC ya mencionados citan las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature- Policy.

3. Tabla sintética de los formularios de CoronApp web (registro, login, reporte)

Categoría	Descripción
URL	https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html
Datos recolectados	• Para el registro: nombre, apellidos, tipo y número de documento, número de celular, correo electrónico, contraseña. • Para el reporte: tipo de síntomas, otros riesgos (contactos, viajes, trabajadores de salud), atención médica recibida o no, detalles sobre los síntomas. Incluye por lo tanto datos sensibles de salud. • Para la conexión a CoronApp web: correo electrónico y contraseña. • Para la obtención del código QR de viaje: fecha del vuelo, tipo de vuelo, aerolínea, número de vuelo, número de silla. [Ver Anexo 5]
Hosting	Igual que en la parte 2, el servidor web principal tenía en nuestro primer análisis la dirección IP 170.246.114.222 que pertenece a la empresa colombiana *Media Commerce Partners S.A.* ubicada en Pereira. Al día de esta publicación tiene la dirección IP 190.145.219.66 que pertenece a la empresa colombiana Telmex Colombia S.A. Como en el caso de la aplicación CoronApp que analizamos anteriormente, tanto los datos personales de los formularios de registro, cómo los datos de reportes de síntomas se envían al dominio "apicovid2.and.gov.co" de la Agencia Nacional Digital. Los servidores web son de *Amazon Technologies* y están ubicados en Estados Unidos (direcciones IP: 3.225.120.50, 3.229.237.212 y 52.54.29.154) [Ver Anexo 5]. Ninguna de estas empresa intermediarias se mencionan en la política de privacidad. **Recomendación: Cómo se explicó en la parte 1, se debería mencionar en la política de protección de datos (tanto en la política general cómo en la política específica de CoronApp_Colombia) la forma como se ha previsto el tratamiento de los datos que incluye terceros que aloja los datos en el exterior. Consideramos que este diseño supone que es una de estas empresas la que está encargada del tratamiento de datos y estas sub-contrataciones implican, como ya vimos, transferencia de datos personales a Estados Unidos.**
Cifrado y autenticación	El portal usa de forma predeterminada el protocolo seguro HTTPS (HTTP+TLS) con certificados válidos de la empresa *Go Daddy Inc*.
Envío de los datos personales	Los datos transmitidos por los tres formularios (registro, conexión y reporte) se envían con el protocolo HTTPS y el método POST. Además se autentica la conexión con un token, hacia el servidor "apicovid2.and.gov.co" y los datos sensibles del cuestionario de reporte de salud, se envían en una forma codificada o cifrada [Ver Anexo 5]. Se confirma por ende que se trabajó para subsanar algunas de las vulnerabilidades que Fundación Karisma había identificado en su primer análisis de CoronApp_Colombia.
Tecnologías usadas y actualizaciones	El servidor web es un servidor Kestrel que usa el framework *Microsoft ASP.NET*. El servidor no deja ver, con un análisis pasivo, las versiones de sus componentes, lo que es bueno desde la mirada de seguridad digital. El análisis de las cookies internas muestra que muy probablemente se usa un balance de carga de tipo "F5 BIG-IP ASM" versión 11.4.0 o posterior [Ver Anexos 4 y 7]. **Recomendación: Es importante asegurarse de la actualización del servidor web y de todos sus componentes.**

Protecciones adicionales	Recomendación: Se recomienda implementar protecciones adicionales, siguiendo los lineamientos de seguridad digital del MinTIC para los sitios web18, en particular las siguientes, ya que nuestro análisis mostró que no están implementadas: Cookies: habilitar atributos de seguridad como *Secure* y *HttpOnly*, en particular para la cookie "TS01bee912" que parece tener funcionalidades de seguridad vinculadas con el balance de carga; 1. Habilitar las cabeceras de seguridad[19].
Verificación de correo y fuga de datos hacia Google y ProjectilesIO	Cuando una persona se registra para usar CoronApp_Colombia, recibe un correo de verificación donde se le pide hacer clic sobre "Confirmar Correo". Al hacer clic sobre este botón, se envía un token de verificación y el correo de la persona se transmite en los parámetros de la URL (método GET). La consecuencia de esta mala práctica es una fuga del token (que afortunadamente sólo funciona una vez) y del correo electrónico hacia los dominios de los terceros "google.com" y "countriesnow.space"[20] Este efecto, que hemos ya mostrado en análisis anteriores de otros sitios del Estado, es una de las razones por las cuales no es recomendable transmitir datos sensibles de esta manera. Esta práctica está prohibida por los lineamientos de seguridad digital del MinTIC para los sitios web[21][Ver Anexo 6]. **Recomendación: dejar de transmitir el correo electrónico en parámetros de la URL para evitar esta fuga de datos a terceros no autorizados. Evaluar el uso de scripts de terceros en la página web de CoronApp_Colombia.**
Rastreo y cookies de tercero	En esta página, se instalan dos cookies de terceros por Google. Esto se deriva del uso del servicio Google Recaptcha ("_GRECAPTCHA") y del dominio "countriesnow.space". Ambas tienen características de cookies de rastreo aunque la segunda tiene finalidades técnicas vinculadas con el hosting del servidor web del dominio en CloudFlare [Ver Anexo 7]. Para la primera, teniendo en cuenta la eficiencia de este servicio en términos de seguridad, se puede entender la decisión de implementarlo, a pesar del rastreo generado por su uso.

18 *Condiciones mínimas técnicas y de seguridad digital del MinTIC* (Anexo 3 de la Resolución MinTIC 1519 del 2020).

19 Los lineamientos del MinTIC ya mencionados citan las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict- Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature- Policy.

20 "countriesnow.space" es un dominio registrado por la organización *ProjectilesIO* y el desarollador Martins Onuoha en Nigeria. El sitio web provee informaciones de localización y generales de los países a través de un archivo JSON, https://countriesnow.space/ y https://documenter.getpostman.com/view/1134062/T1LJjU52?version=latest .

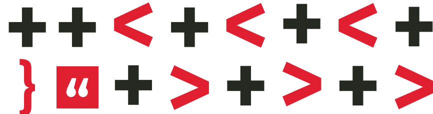
21 Revisar la condición de seguridad n.º 4 ("no enviar parámetros sensibles a través del método get") de las Condiciones mínimas técnicas y de seguridad digital del MinTIC (Anexo 3 de la Resolución MinTIC 1519 del 2020).

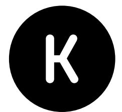
ANEXOS – Referencias técnicas

[1] Datos recolectados y enviados en el auto-diagnóstico

Aquí se presentan el formulario de auto-diagnóstico y el correspondiente paquete HTTP(S) que transmite los datos.

Formulario web https://coronaviruscolombia.gov.co/Covid19/auto-diagnostico.html	**Extracto de la captura HTTP(S) correspondiente (transmisión de estos datos)**
Análisis de síntomas COVID-19 Te haremos unas preguntas para determinar tu riesgo de coronavirus(COVID-19) ¿Has estado en contacto estrecho (cercano), sin usar elementos de protección, por más de 15 minutos con una persona con diagnóstico confirmado de COVID-19? o ¿has estado compartiendo el mismo lugar por más de 120 minutos con una persona con diagnóstico confirmado de COVID-19? Si No ¿Has presentado alguno de estos síntomas recientemente (en los últimos 14 días)? Fiebre de 38°C o más Tos Dificultad para respirar Fatiga o decaimiento Dolor de garganta Disminución del sentido del gusto Disminución del sentido del olfato Ninguno Continuar	***https://api.amplitude.com/*** *POST / HTTP/1.1* ***Host: api.amplitude.com*** *[...]* *Content-Length: 1038* *Origin: https://www.1doc3.com* *Connection: keep-alive* *client=6b2c935524dec5581a8763da80d125a2&e=[{"device_id":"7f40bdf1-4a69-411d-a4b5-1b06fd838f54",**"user_id":"7f40bdf1-4a69-411d-a4b5-1b06fd838f54"**,"timestamp":1612670121469,"event_id":3,"session_id":1612669843002,**"event_type":"Coronavirus test finished"**,"version_name":null,"platform":"Web","os_name":"Firefox","os_version":"56","device_model":"Linux","language":"en-US","api_properties":{},"event_properties":{"category":"All","label":**"Test finished","userCondition":"Tos, Disminución del sentido del gusto","userRiskContact":"No","userDrowned":"No"**},”user_properties”:{},”uuid”:”5c6b657e-317e-4ad0-8f11-3b7dcc8c3234”,”library”:{“name”:”amplitude-js”,”version”:”2.1.0”}}]&v=2&upload_time=1612670121476&checksum=a26a4bbc29aa1545b0f3ede97d9677ae*





En el formulario se recolectan los datos correspondiente al contacto eventual con una persona infectada con COVID-19 y a los síntomas (en el caso de nuestra prueba, *Tos* y *Disminución del sentido del gusto*). El extracto de captura HTTP(S) muestra que se transmiten vía el protocolo seguro HTTPS (con el método POST).

El destinatario de estos datos es el sub-dominio "api.amplitude.com" que pertenece a la empresa *Amplitude* que provee servicios de analítica de datos y está ubicada en Estados Unidos[22]. Esto se explica en el anexo siguiente.

También se puede observar que los datos transmitidos en el paquete y relacionados con el formulario (*"Test finished", "userCondition":"Tos, Disminución del sentido del gusto","userRiskContact":"No","userDrowned":"No"*) están asociados a varios identificadores de las personas que usan los servicios (*device_id*, *user_id* y *uuid*) y a características detalladas del equipo, del sistema operativo y del navegador (lo que puede servir para hacer un cálculo de huella o fingerprint del dispositivo e identificarlo de esta forma).

22 https://amplitude.com/

[2] De la Presidencia hacía “1doc3” y “amplitude.com”

La empresa “1Doc3” y su dominio asociado “1doc3.com” aparece directamente en el sitio web cuando, después de llenar el formulario de auto-diagnóstico, se hace clic en “Conocer más”:



Además, en el código HTML de la página de auto-diagnóstico, se puede observar que el cuestionario es un iframe (un elemento HTML que permite insertar un documento HTML externo) de “1doc3.com”:

```
<iframe src="https://www.1doc3.com/web/coronavirustest?no_actions=true"
frameborder="0" scrolling="yes"
onload="FuncionalidadesGenerales.resizeIframe(this)" title="Realiza tu auto
diagnostico del COVID-19"></iframe>
```

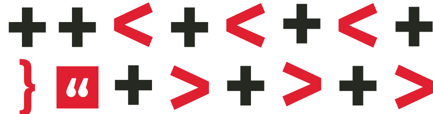
Es decir que es como si la URL real del cuestionario fuera “`https://www.1doc3.com/web/coronavirustest`”.

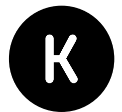
Esto se puede observar también en las capturas HTTP(S) que se analizaron, por ejemplo ésta que es la primera originada desde la página:

```
https://www.1doc3.com/web/coronavirustest?no_actions=true

GET /web/coronavirustest?no_actions=true HTTP/1.1
Host: www.1doc3.com
[...]
Referer: https://coronaviruscolombia.gov.co/Covid19/auto-diagnostico.html
```

La conexión con “amplitude.com” se hace cuando hay una solicitud originada por “1doc3.com” (ver Referer) hacia el siguiente recurso javascript:





https://d24n15hnbwhuhn.cloudfront.net/libs/amplitude-2.1.0-min.js

```
GET /libs/amplitude-2.1.0-min.js HTTP/1.1
Host: d24n15hnbwhuhn.cloudfront.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Waterfox/56.3
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.1doc3.com/web/coronavirustest?no_actions=true
Connection: keep-alive
```

En el código fuente de este script, se puede observar que se origina en seguida la conexión con una API de “amplitude.com”, en el endpoint “api.amplitude,com”:

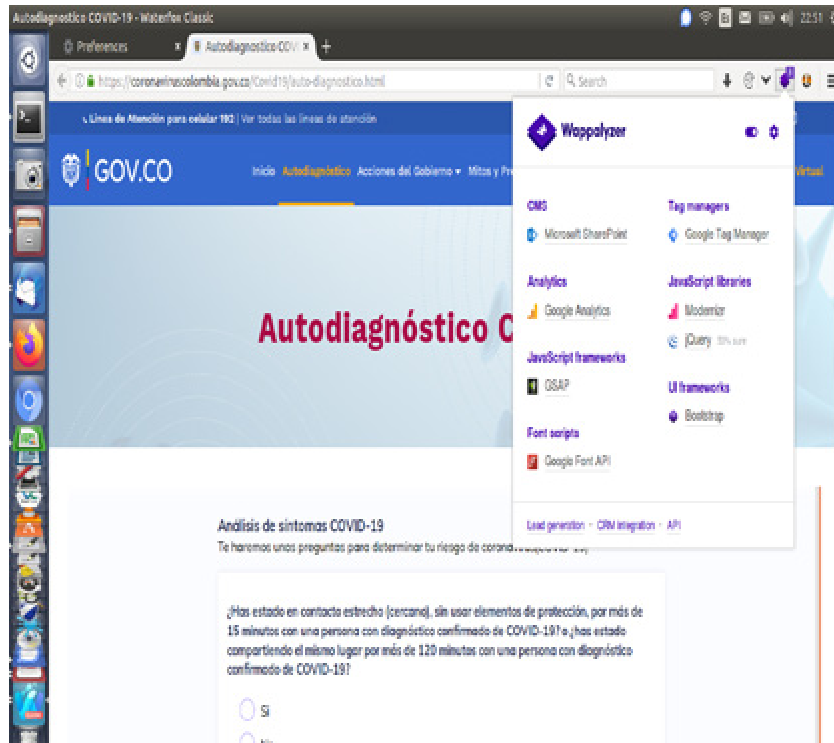
```
apiEndpoint:"api.amplitude.com"
```

Desde la ejecución de esta función javascript (**amplitude-2.1.0-min.js**) se originan varias solicitudes hacia “api.amplitude.com”, entre ellas la que se muestra en el anexo 1 y que transmite los datos a la empresa *Amplitude*.

[3] Tecnologías usadas

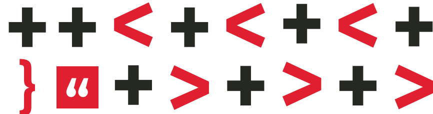
El hecho de que el servidor web sea un servidor Microsoft Share Point se puede observar en ciertas respuestas HTTP del servidor:

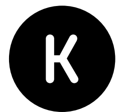
El uso del framework de código abierto Bootstrap, junto con ciertas herramientas, se puede observar por ejemplo con la herramienta Wappalyzer[23] o directamente en el código fuente HTML de la página:




```
<link rel="stylesheet" href="css/vendor/bootstrap.min.css"/>
```

23 https://www.wappalyzer.com/





[4] Cookies instaladas en la página de auto-diagnóstico y otro rastreo

Aquí se pueden observar las cookies instaladas (en el análisis de febrero 2021):

Domain	Name	Content	Expires	HTTP Only	Secure
~~.1doc3.com~~	~~_gat~~	~~1~~	~~6 de febrero de 2021 22:56:21 G...~~	~~No~~	~~No~~
.1doc3.com	ajs_anonymous_id	%22ae26385b-e980-4594-821b-8f6ecff0e1e7%22	6 de febrero de 2022 22:50:43 G...	No	No
.1doc3.com	amplitude_id1doc3.com	eyJkZXZpY2VJZCI6IjdmNDBiZGYxLTRhNjktN...	4 de febrero de 2031 22:50:42 G...	No	No
.facebook.com	fr	0BUO3nkyRCrVgwxEL.BgH2OR...1.0.BgH2OR.	7 de mayo de 2021 22:50:41 GMT-5	Yes	Yes
.1doc3.com	_gid	GA1.2.2125541057.1612669841	7 de febrero de 2021 22:50:41 G...	No	No
.1doc3.com	_ga	GA1.2.1470474299.1612669841	6 de febrero de 2023 22:50:41 G...	No	No
.1doc3.com	ajs_group_id	null	6 de febrero de 2022 22:50:37 G...	No	No
.1doc3.com	ajs_user_id	null	6 de febrero de 2022 22:50:37 G...	No	No
.1doc3.com	undoctres	dldvucdjpeecakopohuu3iuepkrf3pbe	7 de abril de 2021 22:50:30 GMT-5	Yes	Yes
~~.coronaviruscolombia.gov.co~~	~~_gat_gtag_UA_16660818_39~~	~~1~~	~~6 de febrero de 2021 22:51:30 G...~~	~~No~~	~~No~~
.coronaviruscolombia.gov.co	_gid	GA1.3.1290119201.1612669830	7 de febrero de 2021 22:50:29 G...	No	No
.coronaviruscolombia.gov.co	_ga	GA1.3.350195024.1612669830	6 de febrero de 2023 22:50:29 G...	No	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co			At end of session	Yes	No
coronaviruscolombia.gov.co	TS01bee912	0120c7c117ef63d1725e8a64048024a9b17face...	At end of session	No	No
coronaviruscolombia.gov.co			At end of session	Yes	No

Las cookies con nombre "_ga" y "_gid" son asociadas al servicio Google Analytics y sirven para distinguir y rastrear a la persona usuaria24 tanto para el servicio de Google Analytics como para usos publicitarios ulteriores.

Varias de estas cookies tienen características de **cookies de rastreo** (contienen un identificador, tienen una duración de larga vida, la empresa asociada puede hacer rastreo publicitario):

- cookie "fr" del dominio "facebook.com" ;
- cookies "_ga" y "_gid" del servicio Google Analytics, asociadas a los dominios "coronavirus.com" y al dominio "1doc3.com" ;
- cookies "ajs_anonymous_id", "amplitude_id1doc3.com" y "undoctres". Se puede observar el nombre de la primera que contiene "anonymous" y de la segunda que contiene "amplitude", así haciendo otra conexión con la empresa Amplitude. También se puede notar su duración de vida record: ¡hasta el 4 de febrero del 2031!

También se puede observar la instalación de varias **"cookies vacías"** (sin nombre ni contenido) con dominio "coronaviruscolombia.com". Es bastante raro e incluso pensamos en un error en nuestra herramienta de análisis de cookies (*Cookie Manager* +) pero el análisis de los paquetes HTTP confirma su instalación a través de varias instrucciones Set-Cookies, cómo ésta:

```
Set-Cookie: ; HttpOnly
```

Probablemente era un error técnico. En la verificación más reciente ya no aparecen estas cookies.

24 https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage

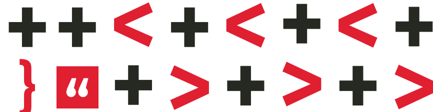
Finalmente, así no se instalen cookies, se observaron varias **solicitudes hacia el dominio publicitario de Google "doubleclick.net",** transmitiendo varios identificadores en los parámetros de la URL (entre ellos la cookie de Google Analytics):

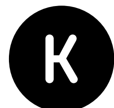
```
https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j87&tid=UA-48707931-1&cid=1470474299.1612669841&jid=546011510&gjid=1771403806&_gid=2125541057.1612669841&_u=aGBAAEACQAAAAC~&z=373993230

POST
/j/collect?t=dc&aip=1&_r=3&v=1&_v=j87&tid=UA-48707931-1&cid=1470474299.1612669841&jid=546011510&gjid=1771403806&_gid=2125541057.1612669841&_u=aGBAAEACQAAAAC~&z=373993230 HTTP/1.1
Host: stats.g.doubleclick.net
[...]
Referer: https://www.1doc3.com/web/coronavirustest?no_actions=true
Content-Type: text/plain
Content-Length: 0
Origin: https://www.1doc3.com
Connection: keep-alive
```

El Referer muestra que fue originado por el dominio "1doc3.com".

Nota: las cookies en rojo son cookies que han sido instaladas y borradas durante el análisis.





[5] Envío de datos en los formularios de registro, login y reporte

Pantallazo formulario	Solicitud HTTP(S) de envío de datos
Nombre * Fundacion Apellidos * Karisma Tipo de documento Cédula de Ciudadanía Número de documento * 1234567890 Número de celular +57 3505943410 Correo ele test4@karisma.org.co Ingresa una contraseña * ********** Acepto los **términos de uso** de CoronApp, para contribuir a la estrategia de prevención del Gobierno Colombiano, frente al Coronavirus. Consulte la **política de tratamiento de la información** de CoronApp. I'm not a robot reCAPTCHA Privacy - Terms Registrarme	**https://apicovid2.and.gov.co/api/v2.0/authentication/register** **POST** /api/v2.0/authentication/register HTTP/1.1 Host: apicovid2.and.gov.co […] Referer: https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html content-type: application/json origin: https://coronaviruscolombia.gov.co Content-Length: 703 Connection: keep-alive {"document_type":"cc","document_number":"**1234567890**","firstname":"**Fundacion**","lastname":"Karisma","email":"**test4@karisma.org.co**","password":"**XXXXXX**","phone":"XXXXX","phone_area_code":"57","recaptcha_token":"03AGdBq26vXd_fmIkrbmbmhrWMKA[…]"} *Nota: En la solicitud real los "XXXXXX" (del teléfono y del password) no eran ofuscados.*
CoronApp Email test4@karisma.org.co Contraseña ●●●●●●●●●●● ¿Olvidaste tu contraseña?	**https://apicovid2.and.gov.co/api/v2.0/authentication/login** **POST** /api/v2.0/authentication/login HTTP/1.1 Host: apicovid2.and.gov.co […] Content-Length: 57 Connection: keep-alive {"email":"**test4@karisma.org.co**","password":"**XXXXXX**"} *Nota: En la solicitud real los "XXXXXX" (del password) no eran ofuscados.*

Selecciona los síntomas que presentas:

- [x] Fiebre
- [ ] Dolor de garganta
- [ ] Congestión nasal
- [x] Tos
- [ ] Dificultad para respirar
- [ ] Fatiga
- [ ] Escalofrío
- [ ] Dolor de músculos
- [ ] Ninguno de los anteriores

Continuar

Elige las opciones que apliquen en tu caso:

- [ ] Estuve en contacto con alguien que tuvo alguno de esos síntomas
- [ ] Hice un viaje internacional en los últimos 30 días
- [x] Hice un viaje nacional en los últimos 30 días
- [ ] Soy trabajador de la salud
- [ ] Ninguna de los anteriores

Continuar

Selecciona los síntomas que presentas:

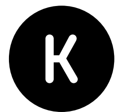
- [x] Fiebre mayor a 37,5°
- [x] Tos reciente o una tos que empeora
- [ ] Leve dificultad para respirar
- [ ] Dificultad para ponerse de pie
- [ ] Mareo
- [ ] Pérdida del gusto o el olfato
- [ ] Diarrea
- [ ] Ninguno de los anteriores

Continuar

(*) Aquí se ponen sólo una parte de las series de preguntas (hay 3 más)

https://apicovid2.and.gov.co/diagnosis/api/v2.0/question

```
POST /diagnosis/api/v2.0/question HTTP/1.1
Host: apicovid2.and.gov.co
[...]
Referer:
https://coronaviruscolombia.gov.co/Covid19/coronApp/diagnostico-coronApp.html
Content-Type: application/problem+json; charset=utf-8
Authorization: Bearer
eyJraWQiOiJNa2FMUHVsVWVFT2lqdGRVYlg0VmMybUc1K2M2R3k3UEtUSngzaU91bWU0PSIsImFsZyI6[….]
Content-Length: 855
Origin: https://coronaviruscolombia.gov.co
Connection: keep-alive
{"fecha":"16/02/2021 15:18:46","diagnostico":
"165389f5-161b-47f2-a7f5-20bed053262d","id_usuario":"602c26f4cf17b300014711 7f","preguntas”:[{“id”:”c9a60560-97b2-47da-9e70-30ca29b98add”,”respuestas”:
[“450de030-b920-4192-be81-0b0b21ae7361”,”a3e3d8ef-98e4-4287-80cd-a1633817fe08”]},{“id”:”cdbc8c94-a47d-4f05-9bb6-b3cde9dd8fcd”,”respuestas”:[“a9a36e37-0c2d-4776-8fee-0e760f8190f8”]},
[…]
:[“f4ca08c5-cdd9-4cb2-8a71-634e0a39b3aa”]}]}
```



Datos del viaje

Fecha de vuelo: 12 - 05 - 2021

Tipo de vuelo: Internacional

Aerolínea: Viva Air

Número de vuelo: VH301

No. silla: 5A

Continuar

```
https://apicovid2.and.gov.co/diagnosis/api/v1.0/travel/createtravelrecord

POST /diagnosis/api/v1.0/travel/createtravelrecord HTTP/1.1
Host: apicovid2.and.gov.co
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://coronaviruscolombia.gov.co/Covid19/coronApp/diagnostico-coronApp.html
Content-Type: application/problem+json; charset=utf-8
Authorization: Bearer eyJraWQiO
[....]
Content-Length: 170
Origin: https://coronaviruscolombia.gov.co
Connection: keep-alive
{"transport_mode_id":1,"airline_id":"16","company_name":"","ship":"VH301","seat":"5A","is_domestic":false,"travel_date":"2021-05-12","origin_mun":"","destination_mun":""}
```

Se puede observar que en los tres casos los datos personales se envían con el protocolo seguro HTTPS y con el método POST. Para los cuestionarios de salud y riesgos frente al COVID-19, se observa la transmisión de un token de autenticación (*Authorization: Bearer*) y las respuestas a las preguntas se hace en una forma codificada o cifrada (por ejemplo: `"respuestas":["450de030-b920-4192-be81-0b0b21ae7361","a3e3d8ef-98e4-4287-80cd-a1633817fe08"]`) excepto en el último formulario. Son buenas medidas desde el punto de vista de la seguridad que corrigen vulnerabilidades que Fundación Karisma había observado en su primer análisis de CoronApp_Colombia.

[6] Correo de verificación y fuga de datos hacia Google y CountriesNow

Después de hacer el proceso de registro uno recibe este correo de confirmación de parte de la Agencia Nacional Digital ("soporte@and.gov.vo"). Es necesario hacer clic en el botón "*Confirmar Correo*" para validar el proceso y activar la cuenta de CoronApp_Colombia para hacer el registro y poder generar un código QR.

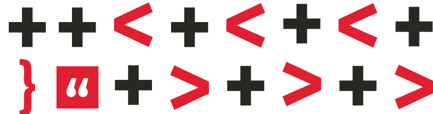


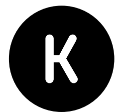
En nuestra prueba, el botón "Confirmar Correo" apuntaba a este link:
`https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html?`**`token=16022021fd377eca8a8f4d64afaca6dda4f6e683`**`&`**`email=test4%40karisma.org.co`**

El link tiene entre sus parámetros un token junto con la dirección de correo[25]. Al hacer clic en este link, estos datos se van a transmitir al servidor web con el método GET. Es una mala práctica desde el punto de vista de la seguridad digital y en este caso, la consecuencia es que estos datos se transmiten a dos dominios externos (presentes en la página web de llegada) vía la cabecera *Referer*: "google.com" (presente en la página por el uso de su servicio RECPATCHA) y "countriesnow.space".

Esto se puede observar en los siguientes paquetes HTTP(S) hacia estos dos dominios:

25 "%40" corresponde al carácter "@" en codificación ASCII/HTML.





```
https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit

GET /recaptcha/api.js?onload=onloadCallback&render=explicit HTTP/1.1
[...]
Referer:
https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html?token=16022021fd377eca8a8f4d64afaca6dda4f6e683&email=test4%40karisma.org.co
Cookie: _GRECAPTCHA=09AGR3LzN0Ex7Bj9lay6Sx2F2Dnf5_wHUdaoV-GePZeKBRuwy6Zquyg70MrT7awICT14PB3Ag6GjPk6TZUXuI-xAk
Connection: keep-alive
```

```
https://countriesnow.space/api/v0.1/countries/codes

GET /api/v0.1/countries/codes HTTP/1.1
Host: countriesnow.space
[...]
Referer:
https://coronaviruscolombia.gov.co/Covid19/coronApp/registro-coronApp.html?token=16022021fd377eca8a8f4d64afaca6dda4f6e683&email=test4%40karisma.org.co
Origin: https://coronaviruscolombia.gov.co
Connection: keep-alive
If-None-Match: W/"33a9-aclBE7bKiE2lKAkbwchP+RLiE3w"
```

[7] Cookies instaladas durante y después del registro a CoronApp_Colombia Web

Durante el registro a la Coronapp_Colombia se instalan estas dos cookies:

Domain	Name	Content	Expires	HTTP Only
.google.com	_GRECAPTCHA	09AGR3LzN0Ex7Bj9lay6Sx2F2Dnf5_wHUdaoV-GePZeKB...	15 de agosto de 2021 15:10:59 G...	Yes
coronaviruscolombia.gov.co	TS01bee912	0120c7c117ca94b77dbbcd8ecc75bf8435e647bf3653d265...	At end of session	No

La primera cookie (“_GRECAPTCHA”), con dominio “google.com” contiene un número de identificación (a priori en Base64) y tiene un fecha de expiración de un año, que es mucho más de lo necesario para su finalidad inicial (protección contra los robots durante la sesión). Tiene las características de una cookie de rastreo y puede ser usada por Google con este fin, más allá de la finalidad de seguridad.

La segunda cookie, interna, (“TS01bee912”) es una cookie de sesión y por lo tanto no implica rastreo. Tiene las características de las cookies de un servidor de balanceo de carga (*load balancing*) de tipo “F5 BIG-IP ASM” con una versión 11.4.0 o posterior[26]. Esta cookie tiene finalidades de seguridad y es por lo tanto sensible[27]. Sin embargo, no tiene habilitados los atributos de seguridad *HTTPOnly* y Secure. Sería necesario hacerlo, siguiendo las recomendaciones de la empresa F5[28] y las recomendaciones de MinTIC para sitios web del Estado[29].

Además, después del proceso de verificación y de conexión, se instala otra cookie llamada “*_cfduid”* y del dominio “countriesnow.space” ya mencionado:

```
set-cookie: __cfduid=d18678fd21da4e4853722c746bde7e0961613506720; expires=Thu,
18-Mar-21 20:18:40 GMT; path=/; domain=.countriesnow.space; HttpOnly;
```

Esta cookie también se debe al hosting del servidor web de este dominio en CloudFlare y tiene finalidades técnicas a pesar de su apariencia de cookie de rastreo[30].

26 “BIG-IP ASM 11.4.0 and later: The ASM Main cookie name structure contains eight hexadecimal characters **(TSxxxxxxxx)**. The first two characters are the revision number and the remaining six characters represent the name of the active security policy.”, Fuente: https://support.f5.com/csp/article/K6850
27 https://support.f5.com/csp/article/K6850
28 Ver aquí en el sitio del constructor para la proceso de configuración: https://support.f5.com/csp/article/K13787
29 *Condiciones mínimas técnicas y de seguridad digital del MinTIC* (Anexo 3 de la Resolución MinTIC 1519 del 2020).
30 https://blog.cloudflare.com/deprecating-cfduid-cookie/

<K+LAB>



karisma.org.co
Twitter: @Karisma
Facebook: @fundacionkarismaa
Instagram: @karismacol